AMENDMENTS TO THE CLAIMS

1. (Currently amended) An apparatus for selectively encrypting data for transmission over a network between a server and a client, the apparatus comprising:

~~means~~ a parser configured ~~for~~ to ~~parsing~~ parse a first portion of the data from a second portion of the data;

~~means for~~ an encrypter configured to ~~encrypting only~~ the first portion of the data; and

~~means for~~ a data combiner configured to ~~combining~~ combine the encrypted first portion of the data with the second portion of the data, wherein the second portion of the data includes more than routing information.

2. (Previously presented) The apparatus of claim 1, wherein the data includes streaming data.

3. (Previously presented) The apparatus of claim 1, wherein the first portion of the data includes payload data.

4. (Previously presented) The apparatus of claim 1, wherein the second portion of the data includes at least one of a header, control data and routing data.

5. (Currently amended) The apparatus of claim 1, further comprising ~~means for~~ a transmitter configured to ~~sending~~ the combined first and second portions of the data over the network to the client.

6. (Currently amended) The apparatus of claim 1, further comprising ~~means for~~ a receiver configured to ~~receiving~~ receive the data from the server before the data is sent over the network to the client.

7. (Currently amended) The apparatus of claim 1, further comprising ~~means for~~ a device configured to ~~establishing~~ a data stream between the server and the client.

8. (Currently amended) The apparatus of claim 1, further comprising <u>a key negotiator</u> <u>configured</u><s>key-negotiating means for</s> <u>to</u> <s>negotiating</s><u>negotiate</u> an encryption key with the client.

9. (Previously presented) The apparatus of claim 8, wherein key negotiation and key exchange occur during transmission of a stream.

10. (Currently amended) The apparatus of claim 9, wherein <u>the encrypter</u> <s>by the</s> <s>encrypting means</s> is transparent to the server.

11. (Currently amended) The apparatus of claim 8, wherein key negotiation can determine <s>the</s><u>a</u> correctness of <s>the</s><u>a</u> result.

12. (Currently amended) The apparatus of claim 1, further comprising <u>a decrypter</u> <u>configured to</u> <s>decrypting means installed at the client for decrypting</s> the first portion of the data.

13. (Currently amended) The apparatus of claim 1, wherein the <s>parsing</s><u>parser is further</u> <u>configured to</u> <s>means</s><u>parses</u> the data into different portions based on <u>a</u> media format.

14. (Currently amended) The apparatus of claim 1, wherein the <u>encrypter is further</u> <u>configured to</u><s>encrypting means</s> <u>encrypts</u> the first portion of the data based on <u>a</u> media format.

15. (Previously presented) The apparatus of claim 1, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the first portion of the data, wherein the pluggable core enables the encryption algorithm to be readily changed.

16. (Currently amended) The apparatus of claim 1, wherein the apparatus in implemented on a<u>n</u> encryption bridge.

17. (Previously presented) A method for selectively encrypting data received from a data source, the data including first and second portions which differ from each other in at least one characteristic, the received data to be subsequently sent over a network to a client, the method comprising:

parsing the received data into portions including the first and second portions;

encrypting the first portion of the received data; and

sending the received data including the encrypted first portion and the second portion of the received data over the network to the client.

18.   (Previously presented) The method of claim 17, wherein the data source is a server.

19.   (Currently amended) The method of claim 17, further comprising determining whether a stream is established between ~~the~~ a_server and the client.

20.   (Currently amended) The method of claim 1~~5~~7, further comprising negotiating an encryption key with the client.

21.   (Previously presented) The method of claim 20, wherein the received data from the data source is streaming data sent during a streaming session and the negotiating of the encryption key is carried out during the streaming session.

22.   (Previously presented) The method of claim 20, wherein the received data from the data source is streaming data sent during a streaming session, the method further comprising examining the client during the streaming session and terminating the streaming session if the encryption key on the client is invalid.

23.   (Previously presented) The method of claim 20, wherein the encryption key is negotiated with a decryption shim on the client.

24.   (Previously presented) The method of claim 17, further comprising determining whether the received data is streaming data.

25.   (Previously presented) The method of claim 24, further comprising parsing, encrypting and sending the data if the data is streaming data and sending the data if the data is not streaming data.

26.   (Previously presented) The method of claim 17, further comprising determining whether a shim is present on the client.

27.   (Previously presented) The method of claim 26, further comprising sending a shim to the client if it is determined that the shim is not present on the client.

28.   (Previously presented) The method of claim 17, further comprising determining whether an encryption key on the client is current.

29.   (Previously presented) The method of claim 17, wherein the data includes a payload data portion and at least one of a header, control data and routing data.

30.   (Previously presented) The method of claim 29, wherein the first portion of the data includes the payload data portion.

31.   (Previously presented) The method of claim 17, wherein the data received from the data source for sending to the client is a stream of packets, the method further comprising determining whether a packet is the last packet in a data stream.

32.   (Previously presented) The method of claim 31, further comprising receiving feedback from a decryption shim on the client if it is determined that the packet is not the last packet in the data stream.

33.   (Previously presented) The method of claim 17, further comprising determining whether the client is compromised.

34.   (Previously presented) The method of claim 33, further comprising continuing parsing, encrypting and sending the data into the first and second portions if it is determined that the client is not compromised.

35.   (Previously presented) The method of claim 33, further comprising terminating the sending to the client if it is determined that the client is compromised.

36. (Previously presented) A method for decrypting streaming data at a client, the data including first and second portions which differ from each other in at least one characteristic, the data having been sent over a network to the client from an encryption source, the encryption source having encrypted the first portion of the data, the method comprising:

  receiving the data sent over the network;

  parsing the data into portions including the first and second portions; decrypting the first portion of the data; and

  passing the decrypted first portion of the data to a higher level of operations for play in the client.

37. (Previously presented) The method of claim 36, further comprising prior to the parsing, determining whether the data is an unencrypted stream.

38. (Previously presented) The method of claim 37, further comprising passing the data to a higher level of operations without parsing and decrypting when it is determined that the data is an unencrypted stream.

39. (Previously presented) The method of claim 36, further comprising negotiating a decryption key with the encryption source.

40. (Previously presented) The method of claim 39, wherein the streaming data is sent from the encryption source during a streaming session and said negotiating the decryption key is carried out during the streaming session.

41. (Currently amended) The method of claim 39, further comprising terminating ~~the~~a stream if the ~~encryption~~ decryption key is invalid.

42. (Previously presented) The method of claim 36, wherein the first portion of the data includes a payload data portion.

43.   (Currently amended) A-The method of claim 36, wherein the data is sent from the encryption source over the network as a stream of data packets, the method further comprising determining whether a packet received by the client is a last packet in a data stream.

44.   (Previously presented) The method of claim 43, further comprising sending feedback to the encryption source if it is determined that the packet is not the last packet in the data stream.

45.   (Previously presented) The method of claim 36, further comprising determining whether the client is compromised.

46.   (Previously presented) The method of claim 45, further comprising continuing the parsing, decrypting and passing the data as aforesaid if it is determined that the client is not compromised.

47.   (Previously presented) The method of claim 45, further comprising terminating a streaming session if it is determined that the client is compromised.

48.   (Previously presented) The apparatus of claim 3, wherein the payload data includes multimedia data.

49.   (Currently amended) The apparatus of claim 1, wherein the parsing-parser means-is further configured to parses the data into different portions based on a data protocol used to transmit the a data stream.

50.   (Currently amended) The apparatus of claim 1, wherein the parsing-meansparser parses the data based on the data protocol.

51.   (Previously presented) The method of claim 41, wherein the terminating of the encrypted stream includes sending a feedback signal to the encryption source instructing to stop sending the data over the network.

52.   (Previously presented) The method of claim 45, further comprising terminating a streaming session based on a determination that the client is compromised.

53.   (Previously presented) A method for selectively encrypting data for transmission over a network, the method comprising examining the data to identify a plurality of portions; at least one of those portions to be to encrypted and at least one of those portions to remain unencrypted, the plurality of portions being combined after such encryption.

54.   (Previously presented) The method of claim 53, wherein the data is received from a data source, wherein the data includes streaming data and wherein the at least one data portion to remain unencrypted includes at least one of a header, control data and routing data.

55.   (Previously presented) The method of claim 54, wherein the streaming data is included in the at least one data portion to remain unencrypted.

56.   (Currently amended) The method of claim 55, further comprising:

        transmitting the combined data over the network to a client; and

        negotiating and exchanging a key with the client before the combined data is transmitted over the network to the client, the key enabling the client to decrypt the encrypted portion of the data for play on the client.

57.   (Previously presented) The method of claim 56, wherein the streaming data is sent during a streaming session and wherein the negotiating and exchanging the key is carried out during the streaming session.

58.   (Previously presented) The method of claim 57, further comprising examining the client during the streaming session and terminating the streaming session if the key on the client is invalid.

59.   (Previously presented) The method of claim 58, wherein the data source is a server and the examining is carried out on an encryption bridge between the server and the network so that the examining of the data, encrypting and combining of the plurality of data portions is transparent to the server.

60.   (Previously presented) The method of claim 59, wherein the key negotiating and exchanging and the decryption using the key is carried out using a shim on the client, the shim being configured so that the negotiating and exchanging of the key thereby and the decrypting of the data thereby is transparent to the client.

61.   (Currently amended) ~~The~~ An apparatus for selectively encrypting streaming data received from a streaming data source for transmission over a network to a client, the apparatus comprising:

> a parser configured to parse a plurality of portions of the streaming data;

> an encrypter configured to encrypt at least one of the plurality of data portions but not encrypt at least one other data portion of the plurality of data portions; and

> a data combiner configured to combine the at least one encrypted data portion with at least one unencrypted data portion.

62.   (Currently amended) The ~~method~~ apparatus of claim 61, further comprising a negotiator, wherein the negotiator ~~negotiating~~ negotiates and ~~exchanging~~ exchanges a key with the client before the combined data is transmitted over the network to the client, the key enabling the client to decrypt the at least one encrypted portion of the data for play on the client.

63.   (Currently amended) The ~~method~~ apparatus of claim 62, wherein the streaming data is sent from the streaming data source during a streaming session and wherein the negotiating and exchanging of the key is carried out during the streaming session.

64.   (Currently amended) The apparatus of claim 63, further ~~comprising~~ configured to perform actions including examining the client during the streaming session and terminating the streaming session if the client has been compromised.

65.   (Currently amended) The apparatus of claim 61, wherein ~~the~~ a second portion of the data includes at least one of a header, control data and routing data.

66.   (Previously presented) The apparatus of claim 61, wherein the streaming data source is at least one server.

67.   (Currently amended) ~~The~~ An apparatus for selectively encrypting data received from a data source for transmission over a network to a client, comprising:

a parser configured to parse at least two portions of the data, at least one of the two portions of the data including more than routing information for ~~the~~ a packet;

an encrypter configured to encrypt only one portion of data not including the routing information for the packet; and

a data combiner configured to combine the parsed at least two portions of the data following encryption of the one portion of data not including the routing information for the packet.

68.   (Previously presented) The apparatus of claim 67, wherein the unencrypted portion of the data includes at least one of a header and control data.

69.   (Previously presented) The apparatus of claim 68, wherein the parser parses the data into different portions based on a data protocol used to transmit the data.

70.   (Currently amended) The apparatus of claim 68, wherein the portion of the data to be encrypted includes media data encoded in a media format and wherein the encrypter encrypts the data to be encrypted based on the media format.

71.   (Currently amended) The apparatus of claim 70, wherein the apparatus is implemented utilizing an application that includes a pluggable core encoding an encryption algorithm for encrypting the data, the pluggable core being replaceable to enable the encryption algorithm to be readily changed.

72.   (Previously presented) The apparatus of claim 71, wherein the apparatus is implemented on an encryption bridge.

73.   (Currently amended) An apparatus for selectively encrypting data received from a data source during a downloading operation, the data being received from the data source for transmission over a network to a client receiving the downloaded data, comprising:

a parser configured to parse at least two portions of the data;

an encrypter configured to encrypt only one of the portions of data; and

a data combiner configured to combine the encrypted portion of data with ~~the~~ an unencrypted portion of data for transmission over the network.

74.   (Previously presented) The apparatus as defined in claim 73, wherein the downloaded data is included in the encrypted portion of the data.

75.   (Previously presented) The apparatus of claim 74, wherein the unencrypted portion of data includes at least one of a header, control data and routing data.

76.   (Currently amended) The ~~method~~ apparatus of claim 75, further comprising a key negotiator configured to perform actions including negotiating and exchanging a key with the client before the data is sent over the network to the client, the key enabling the client to decrypt the encrypted portion of data.

77.   (Currently amended) The ~~method~~ apparatus of claim 76, wherein the data is sent during a downloading operation and wherein the negotiating and exchanging of the key is carried out during the downloading operation.

78.   (Currently amended) An apparatus for selectively encrypting data, received from a data source during a downloading operation and for selectively encrypting data received from a data source during a streaming operation, the data being received from the data source for transmission over a network to a client receiving the downloaded or streaming data, comprising:

        a means for ~~parser~~ parsing ~~configured to parse~~ at least two portions of the data;

        a means for encrypting~~an encrypter configured to encrypt~~ only one of the at least two portions of data; and

        a means for combining~~and a data combiner configured to combine~~ the encrypted portion of the data with the at least the unencrypted portion of the data for transmission over the network.

79.   (Currently amended) The apparatus of claim 78, wherein during ~~a~~ the streaming operation, the streaming data is included in the data portion that is to be encrypted.

80.   (Currently amended) The apparatus as defined in claim 79, further comprising a key negotiator, the negotiator being negotiating means configured to negotiate and exchange a key with the client before the streaming data is sent over the network to the client, the key enabling the client to decrypt the encrypted portion of the data for play on the client.

81.   (Currently amended) The apparatus as defined in claim 80, wherein the streaming data is sent during a streaming session and wherein said key negotiator negotiating means is configured to negotiate and exchange the key during the streaming session.

82.   (Currently amended) The method apparatus of claim 81, further comprising a client examiner examining means configured to examine the client during the streaming session and terminate the streaming session if the client has been compromised.

83.   (Previously presented) The apparatus of claim 82, wherein the data portion that is not encrypted includes at least one of a header, control data and routing data.

84.   (Previously presented) The apparatus of claim 78, wherein during a downloading operation, the downloaded data is included in the data portion that is to be encrypted.

85.   (Previously presented) The apparatus of claim 84, wherein the data portion that is not encrypted includes at least one of a header, control data and routing data.

86.   (Previously presented) A shim deployed on a client, the shim comprising:
        a data receiver configured to receive partially encrypted data transmitted to the client;
        a parser configured to parse the partially encrypted data to select a portion of the data to be decrypted;
        a decrypter configured to decrypt the portion of the data selected for decrypting by the parser; and
        a data transmitter configured to send the decrypted data to a higher level operation resident on the client.

87.   (Currently amended) The shim of claim 86, wherein the an encrypted portion of the transmitted data includes media data, the data transmitter being further configured to send the decrypted media data to a media player resident on the client.

88.   (Previously presented) The shim of claim 87, wherein the media data is streaming media transmitted to the client during a streaming session.

89.   (Currently amended) The shim of claim 88, wherein the unencrypted portion of the data includes at least one of a header, control data and routing data.

90.   (Currently amended) The shim of claim 88, further comprising an analyzer configured to analyze the a behavior of the client to detect known media piracy techniques and to terminate the streaming session if a known media piracy technique is detected.

91.   (Currently amended) The shim of claim 88, further comprising an analyzer configured to analyze the a behavior of the client to detect suspicious client behavior and to terminate the streaming session if specific behavior is detected.

92.   (Currently amended) The shim of claim 88, further comprising an analyzer configured to analyze the a behavior of the client to detect known media piracy techniques and to terminate operation of at least the decrypter when a media piracy technique is detected.

93.   (Currently amended) The shim of claim 88, further comprising an analyzer configured to analyze the a behavior of the client to detect suspicious client behavior and to terminate the operation of at least the decrypter if suspicious behavior is detected.

94.   (Previously presented) The shim of claim 88, further comprising a key negotiator configured to negotiate and exchange a key with the client before the data is sent over the network to the client, the key enabling the client to decrypt the encrypted portion of the data for play on the client.

95.   (Currently amended) The shim of claim 88, wherein the streaming data is sent to the client from an encryption source, the shim further including a key negotiator configured to

negotiate and exchange a key with the encryption source, the key being used by the decrypter to decrypt the encrypted portion of the data.

96.   (Previously presented) The shim of claim 95 wherein the key negotiator is further configured to carry out the negotiating and exchanging of the key with the encryption source during the streaming session.

97.   (New) A method for providing selectively encrypted data over a network, comprising:

        determining a plurality of portions of the data;

        selectively encrypting at least one portion in the plurality of portions, wherein at least one other portion remains unencrypted;

        authenticating a client to receive the selectively encrypted portion; and

        transmitting the selectively encrypted portion to the authenticated client.

98.   (New) The method of claim 97, wherein authenticating the client further comprises the client accepting a shim transmitted from a server that is selectively encrypting the portion, and wherein the shim is configured to send back a confirmation.

99.   (New) The method of claim 97, wherein authenticating the client further comprises the client transmitting a self-generated certificate.